

### **REMARKS**

Claims 1, 2, and 4-23 are pending in this application.

Applicants have amended claims 1, 7, 8, 13, 15-19, 21, and 23.

The changes to the claims made herein do not introduce any new matter. In particular, the feature recited in amended claims 1, 13, and 18 that “the terminal only requires the user to make the personal feature accessible to the terminal, or enter the personal feature at the terminal, after the terminal has presented the secret to the user” finds support at least in Paragraphs [0015] and [0033] of the published specification (see US 2007/0185811 A1), as well as in Figure 2B. A similar recitation has been added to the other independent claims. The element recited in the amendment to claims 21 and 23 finds support at least in Paragraph [0045] of the published specification.

#### **Rejection Under 35 U.S.C. § 101**

Claims 15-17 have been rejected under 35 U.S.C. § 101 as being directed toward non-statutory subject-matter. In Paragraph 10 of the Final Office Action, the Examiner states that this rejection would be overcome by expressly reciting that the modules of claims 15-17 are embodied on a non-transitory computer readable medium.

Without any admission as to the propriety of the rejection, and solely to expedite allowance of the subject application, Applicants have amended claims 15-17 in accordance with the Examiner’s suggestion. Accordingly, Applicants request that the rejection of claims 15-17 under 35 U.S.C. § 101 be withdrawn.

#### **Rejection under 35 U.S.C. § 112**

Applicants respectfully request reconsideration of the rejection of claims 15-17, 21, and 23 under 35 U.S.C. § 112, second paragraph, as being indefinite.

As set forth above, Applicants have amended claims 15-17 to specify that the modules recited in these claims are embodied on a non-transitory computer readable medium. Thus, as

stated by the Examiner (see Paragraph 10 of the Final Office Action), present claims 15-17 satisfy the definiteness requirement of 35 U.S.C. § 112, second paragraph.

With regard to claims 21 and 23, Applicants have amended each of these claims to clarify the claimed subject matter. In particular, claims 21 and 23 have been amended to specify that the secret is “information suitable for proving to the user that there has been a successful authentication of the terminal at the background system.” Applicants respectfully submit that present claims 21 and 23 satisfy the definiteness requirement of 35 U.S.C. § 112, second paragraph.

Accordingly, in view of the foregoing, Applicants request that the rejection of claims 15-17, 21, and 23 under 35 U.S.C. § 112, second paragraph, be withdrawn.

#### Rejections Under 35 U.S.C. § 103

Claims 1-19 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Lai On* (US 2002/0059531 A1) in view of *Schneier* (Handbook of Applied Cryptography) and *Kitada* (US 2003/0037163 A1).

Applicants respectfully request reconsideration of the obviousness rejection. As will be explained in more detail below, the combination of the *Lai On*, *Schneier*, and *Kitada* references would not have rendered the subject matter defined in claims 1, 2, and 4-19, as presented herein, obvious to a person having ordinary skill in the art.

#### Independent Claims

In the field of electronic transactions, a user typically authorizes a transaction by entering a personal feature at a terminal. The personal feature may be, for example, a PIN or a fingerprint. However, a possible attacker might set up a counterfeit terminal that looks confusingly like a genuine terminal, but records and misappropriates the user's personal feature data.

The present invention allows the user to reliably convince himself/herself of the integrity of a terminal before the user needs to present any personal feature (such as, for example, a fingerprint) to the terminal. In this respect, the present invention uses a secret that is known to the user, and that signals to the user that the terminal can be trusted. As recited in present claims 1, 13, and 18, ‘the terminal only requires the user to make the personal feature accessible to the terminal, or enter the personal feature at the terminal, after the terminal has presented the secret to the user” (emphasis added). In other words, the terminal first presents the secret to the user, thus signaling to the user that the terminal can be trusted, and only thereafter requires the user to present his or her personal feature to the terminal.

In Paragraph 20 of the Final Office Action, the Examiner relates the recitation of the independent claims to the teachings of *Lai On*. However, Applicants respectfully submit that the Examiner’s assessment does not do full justice to the claim language. For example, in item “k” of Paragraph 20, the Examiner has not given any justification for the alleged teaching of *Lai On* that presenting data to the user (presumably the session key) serves to signal to the user that the terminal can be trusted, as claimed. Applicants submit that, in fact, there is no teaching in *Lai On* to this effect.

Furthermore, in item “j” of Paragraph 20, the Examiner regards the “Second Site’s Site Key” of *Lai On* as data pertaining to a secret that is known to the user. However, the only secret of *Lai On* is the user password or user biometric that is disclosed in Paragraph [0020]. *Lai On* discloses in Figure 3 at step 303 that the Second Site’s Site Key is generated by the authentication site. Thus, the Second Site’s Site Key does not pertain to the user’s confidential login information or biometric, but is newly generated information which is different from any secret of the user.

It is therefore submitted that *Lai On* does not teach any secret data that pertains to a secret known to the user, wherein the secret is presented to the user, thus signaling to the user

that the terminal can be trusted. In particular, the various keys taught by *Lai On* are just used for authentication purposes within *Lai On*'s system. There is no teaching in *Lai On* that these keys are at all presented to the user. However, even if it were to be assumed that one of these keys may appear, say, in the address field of the user's browser, then this key is presumably just a long sequence of numbers and letters that will be utterly meaningless to the user. It can not be reasonably said that a meaningless character sequence signals anything to the user, much less signals to the user that the terminal can be trusted.

Yet further, claims 1, 13, and 18 have been amended to recite that "the terminal only requires the user to make the personal feature accessible to the terminal, or enter the personal feature at the terminal, after the terminal has presented the secret to the user." The other independent claims have been amended similarly. This feature directly contradicts the following teaching of *Lai On*. According to *Lai On*, the user must enter confidential information (such as a user password or a user biometric) at the first vendor site *as the very first step of the process, i.e.*, in step 301 shown in Figure 3. Therefore, in the system of *Lai On*, there is no provision whatsoever that would allow the user to convince himself/herself of the integrity of a terminal before needing to enter confidential information. The system of *Lai On* therefore has exactly the disadvantage that is addressed by the present application. Applicants submit that the present invention can not reasonably be regarded as being obvious from the system of *Lai On* that is not at all concerned about the goal of protecting the user's confidential information from being spied out by possibly fraudulent terminals.

The other cited references cannot cure the deficiencies of *Lai On*. In Paragraph 22 of the Final Office Action, *Schneier* was cited as allegedly teaching the use of secret keys for encrypted communications. However, the use of safe encrypted communications, although important in the context of the present invention, does not have much relevance with respect

to the basic idea of the present invention to allow the user to convince himself/herself of the integrity of a terminal before needing to enter confidential information.

In Paragraph 23 of the Final Office Action, *Kitada* was cited as allegedly disclosing a terminal that sends authentication information to an authentication server. However, the mere step of authenticating a terminal is not sufficient to render the presently claimed subject matter obvious to the ordinarily skilled person. Even if an authentication step were to be added to the system of *Lai On*, then the combination of *Lai On*, *Schneier*, and *Kitada* would still not teach at least the claimed elements of (i) presenting the secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted, and (ii) wherein the terminal only requires the user to make the personal feature accessible to the terminal, or enter the personal feature at the terminal, after the terminal has presented the secret to the user. Thus, even the combination of *Lai On*, *Schneier*, and *Kitada* would still not result in a system according to the present invention, which allows the user to convince himself/herself of the integrity of a terminal before the user is required to enter confidential information.

Accordingly, independent claims 1, 8, 13, and 15-19, as presented herein, are patentable under 35 U.S.C. § 103(a) over the combination of *Lai On* in view of *Schneier* and *Kitada*.

#### Dependent Claims

Each of dependent claims 2 and 4-7 depends from independent claim 1. Each of dependent claims 9-12 ultimately depends from independent claim 8. Dependent claim 14 depends from independent claim 13. All of the present dependent claims are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Lai On* in view of *Schneier* and *Kitada* for at least the reason that each of these claims ultimately depends from one of the present independent claims.

Rejection of Claims 20 and 22

Claims 20 and 22 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Lai On* in view of *Schneier* and *Kitada*, and further in view of *Noguchi* (US 7,215,775 B2). Claims 20 and 22 depend from independent claims 1 and 8, respectively. The *Noguchi* reference does not cure the above-discussed deficiencies of the combination of the *Lai On*, *Schneier*, and *Kitada* references relative to the subject matter defined in present independent claims 1 and 8. Dependent claims 20 and 22 are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Lai On* in view of *Schneier*, *Kitada*, and *Noguchi* for at least the reason that each of these claims depends from either claim 1 or claim 8.

Claims 21 and 23

The Examiner has not addressed the substance of dependent claims 21 and 23 in the Final Office Action, presumably due to the rejection of these claims under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Claims 21 and 23 have been amended and now further emphasize the feature that the secret that is presented to the user is information suitable for proving to the user that there has been a successful authentication of the terminal at the background system. None of the keys of *Lai On*, which presumably are just unintelligible character sequences, can possibly serve to provide any meaningful information to the user, let alone to prove to the user that there has been a successful authentication of the terminal at the background system, as claimed. Thus, for at least this reason, dependent claims 21 and 23 are patentable under 35 U.S.C. § 103(a) over the prior art of record.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 2, and 4-23, as amended herein, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the

Application No. 10/579,961  
Amendment dated June 21, 2011  
Response to Final Office Action mailed December 22, 2010  
(Submitted with RCE)

Examiner may reach the undersigned at (408) 749-6902. If any additional fees are due in connection with the filing of this paper, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP011).

Respectfully submitted,  
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine  
Reg. No. 32,043

710 Lakeway Drive, Suite 200  
Sunnyvale, California 94085  
**Customer Number 25920**